RFC-0007 Significant Change Notification Standard

Thursday, April 24, 2025

Background

OMB Circular A-130: Managing Information as a Strategic Resource Appendix I states *"under ongoing authorization, reauthorization is typically an event-driven action initiated by the authorizing official or directed by the Risk Executive (function) in response to an event or significant change that increases information security or privacy risk above the previously agreed-upon agency risk tolerance."*

NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy Appendix F similarly states that *"under ongoing authorization, reauthorization is in most instances, an event-driven action initiated by the authorizing official or directed by the senior accountable official for risk management or risk executive (function) in response to an event that results in security and privacy risk above the level of risk previously accepted by the authorizing official."* This section also states that *"Organizations establish criteria for what constitutes significant change based on a variety of factors."*

The FedRAMP Authorization Act (44 USC § 3609 (a) (7)) directs the Administrator of the General Services Administration to *"coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the [OMB] Director and the [DHS] Secretary, to establish and regularly update a framework for continuous monitoring..."* This responsibility is delegated to the FedRAMP Director.

Introduction

This FedRAMP standard moves away from the historical presumption that all significant changes to FedRAMP authorized cloud service offerings require prior federal approval and reauthorization by a "lead agency." Agencies must follow OMB policy and NIST standards when adopting FedRAMP authorized cloud services, including performing a full review and risk assessment based on the materials within a FedRAMP authorization package.

FedRAMP asserts that authorization to operate a cloud service establishes an agreed-upon agency risk tolerance that expects the provider to continuously improve the service without triggering reauthorization for most significant changes, and that third-party assessment organizations provide the necessary rigor to identify the risks of such changes on behalf of the authorizing officials. FedRAMP further asserts, as a program responsible for a government-wide approach to the use of cloud services, that no single agency should block improvements to shared services when those improvements may be used by other agencies.

This updated standard creates a new Significant Change Notification standard that replaces all previous FedRAMP guidance related to Significant Change Requests for all FedRAMP authorizations and certifications, including the current Rev 5 Agency Authorization process and FedRAMP 20x. Best practices and technical assistance to help stakeholders follow this standard will be provided separately.

This standard does not supersede any agreement signed between a federal agency and a cloud service provider that sets additional requirements beyond those required by FedRAMP.

Definitions

The following definitions apply to all FedRAMP materials:

a. "**Significant change**" has the meaning given in NIST SP 800-37 Rev. 2 or any successor document. As of April 2025 that means "a change that is likely to substantively affect the security or privacy posture of a system."

    1. FedRAMP excludes routine recurring activities that are part of ongoing operations or vulnerability mitigation and remediation from the criteria for determining significant changes. Such changes are NOT considered significant changes for the purposes of this standard.

b. "**Adaptive change**" means any significant change that adjusts existing components or functionality of the cloud service offering. This is the least impactful type of significant change.

c. "**Transformative change**" means any significant change that adds, replaces, or removes major components and functionality of the cloud service offering.

d. "**Impact categorization change**" means any significant change that is likely to increase or decrease the impact level rating for the cloud service (e.g. from low to moderate or from high to moderate). This is the most impactful type of significant change.

Significant Change Notification Standard

The FedRAMP Significant Change Notification (SCN) Standard establishes standard requirements that cloud service providers MUST follow to maintain FedRAMP authorization when making significant changes to FedRAMP authorized cloud services.

1. Providers MUST NOT make impact categorization changes via the FedRAMP significant change process; security objective changes require re-authorization.

2. Providers MUST follow the procedures documented in their security plan to plan, test, perform, assess, and document changes.

3. Providers MUST assess all planned changes to determine if they may be a significant change.

4. Providers MUST determine if the significant change is an adaptive change, a transformative change, or an impact categorization change, and follow appropriate procedures; providers MUST use the most impactful significant change type that likely applies.
5. Providers MUST keep historical significant change notifications available to agency customers until the service completes its next annual assessment.
6. Providers MUST maintain auditable records of these activities and make them available to FedRAMP, agencies, and contracted 3PAOs.
7. Providers MUST make ALL significant change notifications and related audit records available in similar human-readable and compatible machine-readable formats.
8. All parties SHOULD follow FedRAMP's best practices and technical assistance on significant change assessment and notification where applicable.

If the significant change is an **adaptive change**, also:

9. Providers MUST notify FedRAMP and agency customers within 14 calendar days AFTER making adaptive changes.
10. Providers MUST notify agency customers at the next monthly monitoring meeting AFTER making adaptive changes.

If the significant change is a **transformative change**, also:

9. Providers MUST have a 3PAO review the scope and impact of the planned change BEFORE making significant changes; providers MUST NOT proceed with significant changes without 3PAO concurrence.
10. Providers MUST work with a 3PAO to develop a security assessment plan BEFORE making transformative changes.
11. Providers MUST discuss the planned change during two sequential monthly monitoring meetings BEFORE making transformative changes.

12. Providers MUST notify FedRAMP and agency customers at least 14 calendar days in advance of the first monthly monitoring meeting BEFORE discussing planned transformative changes.

13. Providers MUST notify FedRAMP and agency customers within 1 calendar day AND at the next monthly monitoring meeting AFTER making transformative changes.

14. Providers MUST have a 3PAO begin assessment of the results no later than 1 calendar day AFTER making transformative changes; this assessment SHOULD be completed within 7 calendar days AFTER making transformative changes.

15. Providers MUST publish updated service documentation and other materials to reflect transformative changes within 3 calendar days AFTER making transformative changes.

16. Providers SHOULD automatically OPT OUT agency customers of transformative changes where possible and appropriate.

17. Providers SHOULD delay or roll back change implementation based on significant increases in unmitigated risk that exceed their documented thresholds.

Application of the Significant Change Notification Standard

Cloud service providers may notify FedRAMP and agencies in a variety of ways as long as the mechanism for notification is clearly documented and easily accessible.

A. Providers MUST follow additional requirements related to significant changes that are part of a contractual or other agreement with specific agency customers.

B. Providers SHOULD be responsive to agency customer requests for additional information, standardized formatting, delivery mechanisms, and other

requests that improve the agency's experience and ability to assess the security of a system.

C. Providers and 3PAOs SHOULD follow the guidelines and best practices in any technical assistance provided separately by FedRAMP regarding the application of the Significant Change Notification Standard.

D. 3PAOs MUST independently notify FedRAMP when Providers do not follow this standard appropriately.

E. Agencies SHOULD use the assessment and information provided in the significant change notification to make continuing authorization decisions regarding the cloud service offering.

F. Agencies SHOULD provide concerns directly to the provider during continuous monitoring meetings in advance of transformational changes or in writing after an adaptive change.

Exceptions to the Significant Change Notification Standard

Cloud service providers MAY be required to delay significant changes beyond the standard notification period and/or be required to submit significant changes for review by FedRAMP or an Authorizing Official as a condition of a formal FedRAMP Corrective Action Plan or other agreement with a federal agency.

Significant Change Notification Requirements

All Significant Change Notifications MUST include at least:

- Service Offering FedRAMP ID
- 3PAO Name (if applicable)
- Type of change (CSP definable)
- Related POA&M (if applicable)
- Short description of change

- Reason for change
- Summary of service components and controls affected
- Copy of the business or security impact analysis (including 3PAO concurrence, if applicable)
- Name and title of approver

Cloud service providers MAY include additional relevant information in Significant Change Notifications.

Adaptive Changes

Significant Change Notifications for adaptive changes MUST ALSO include at least:

- Date of Change
- Summary of steps that were taken to verify and assess controls after implementation
- Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)

Transformative Changes

Significant Change Notifications sent BEFORE transformative changes MUST ALSO include at least:

- Planned change date
- Rollback plan (high level)
- If the change is opt in, include the risk associated with the change even if the agency does not opt in
- How to opt in (if applicable)
- Steps that will be taken to verify and assess controls after implementation
- Detail on service components and controls affected
- Copy of the security assessment plan

Significant Change Notifications sent AFTER transformative changes MUST ALSO include at least:

- Date of Change
- Steps that were taken to verify and assess controls after implementation
- Summary of any new risks identified and/or POA&Ms resulting from the change (if applicable)
- Copy of the security assessment report